CHAPTER

3

PLANNING AN ACTIVE DIRECTORY IMPLEMENTATION

After completing this chapter, you will be able to:

- Choose an appropriate organizational model within Active Directory
- Plan the DNS namespace for the Active Directory enterprise
- Understand the use of sites and site boundaries within Active Directory
- Design for flexibility of organizational or geographic changes
- Understand the use of Organizational Units within Active Directory
- Design an appropriate infrastructure for the Active Directory enterprise

Planning has always been a large part of any network design. It is particularly crucial for you to understand the business needs driving the creation of the network and the capabilities of the technology that is implemented. It seems simplistic to state that "planning is the first job," but too often network systems are built in a haphazard manner. Windows NT seems particularly vulnerable to "evolution networking" due to the standalone character of domains. In addition, the ease of installation and administration within Windows NT often leads to inexperienced administrators controlling the systems.

The integration of directory services with Windows 2000 places a much higher premium on planning and analysis skills. Some factors simply must be resolved before the first CD is placed in a drive—for example, DNS namespace issues, whether to implement a single domain or a multiple-domain tree, and how best to organize the company structure. We will examine some of these issues throughout the course of this chapter.

NAMESPACE

One of the most significant issues surrounding the implementation of Active Directory is how best to implement the new namespace. Windows 2000 uses Domain Name System (DNS) as a primary method of name resolution, and the specific Windows 2000 implementation of DNS is tied directly to the directory services within Windows 2000. This use of DNS leads to two separate but intertwining issues: how best to integrate Active Directory into an existing DNS namespace, and how best to implement Windows 2000 DNS.

The specifics for installing and implementing Windows 2000 DNS are covered in Chapter 4 of this book. Our discussion in this chapter will cover planning and the impact of the various methods of namespace design.

Essentially, you have two options when it comes to planning an Active Directory implementation. The first option is to create an entirely new namespace specific to the Active Directory. The second option is to integrate Active Directory into an existing DNS namespace. Both approaches offer advantages and disadvantages, as detailed in the following sections.

New DNS Namespace

Companies often create a new DNS namespace when they have not been using DNS for internal name resolution. This is very often the case when you are upgrading a Windows NT environment, because of the use of Windows Internet Naming Service (WINS) name resolution within Windows NT networks. A new DNS namespace is also useful when you need internal and external resources to be clearly delineated. A separate namespace for internal and external resources allows a clear separation of administrative and logical structures.

DNS namespaces must be registered with an Internet Corporation for Assigned Names and Numbers (ICANN)-approved registrar—even namespaces that you will be using for internal use only. Registration of the domain name (microsoft.com, for example) allows your company to control the namespace and prevents others from using that namespace.

Often, companies will use different namespaces for internal and external resources. Resources available to the public (such as HTTP or FTP servers) will be part of a public namespace, whereas domain controllers (DCs) and file servers will be part of a second, private namespace. In most cases, at least two DNS servers will be involved: The DNS server that provides resolution for the external namespace either will be hosted by a connectivity provider or will be located outside a company's firewall, whereas the server for the internal DNS will be located within the firewall and maintained by the network administrators. An example of this form of configuration is

shown in Figure 3-1. Usually, the second namespace is not published to the external world. The advantages of this configuration are the following:

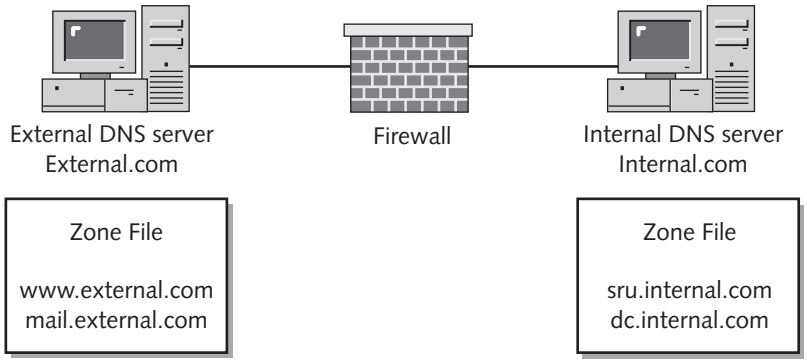

Figure 3-1 Separate DNS namespaces

- You can easily separate internal and external resources. The domain name makes it easy to differentiate between internal and external servers.
- Administration is separated for internal and external namespaces. For many businesses, the connectivity provider administers the external DNS namespace, whereas network administrators handle the internal DNS namespace.
- You can easily secure the internal resources. Firewalls, proxy servers, or other security devices can disallow external traffic bound for the internal namespace, and the internal namespace does not need to be published outside the company.
- If your company has a restrictive Internet access policy, clients can be granted access only to the internal resources through several methods: firewall filtering rules, proxy server configurations, publishing only internal DNS namespaces, or Web browser configurations.

Naturally, maintaining separate internal and external DNS namespaces has disadvantages. Most of the disadvantages are administrative issues:

- *The company must maintain seperate DNS name tables for each name space*. Although the automated features of Windows 2000 Dynamic Domain Name Service (DDNS) help alleviate that burden on the internal namespace, someone must maintain and administer both namespaces individually.
- *The company must maintain and pay for multiple domain name registrations*. Although the cost of registering and maintaining domain name registrations has fallen lately, a slight administrative cost is related to this activity.
- *Logon names will be different from Internet e-mail addresses*. This difference can be an issue if it confuses the user base. You may need to provide some user education.

Integration with an Existing Namespace

Sometimes a new namespace is not a viable option for a company. A company may already be using DNS for internal name resolution, or it may simply resist the idea of multiple namespaces. In this case, Windows 2000 name servers can be integrated into the existing namespace.

You can use two separate methods to integrate Active Directory into an existing DNS environment:

- *Integrate Active Directory at the root level*. For example, using this approach, server.domain.com and workstation.domain.com are included within the same zone as the publicly accessible resources such as **www.domain.com**.
- *Define a subdomain of the root domain and then install the Active Directory tree within that subdomain*. Doing so would result in server.subdomain.domain.com and workstation.subdomain.domain.com, and would allow the administrator to use firewall filtering and custom zone files to protect these machines from external attack. In most cases, Windows 2000 installations that are integrated with existing DNS structures will be configured as subdomains of the existing DNS namespace.

Just as a separate, nonpublic namespace helped protect the internal resources in our earlier example, a separate, nonpublic zone helps protect internal resources when extending a namespace. As shown in Figure 3-2, two DNS servers are separated by a firewall, proxy server, or other security device. The externally accessible DNS server has a zone file that includes information only about resources that the public should be able to access. The internal DNS server has a zone file that also includes information about the internal structure of the network and the locations of the internal resources.

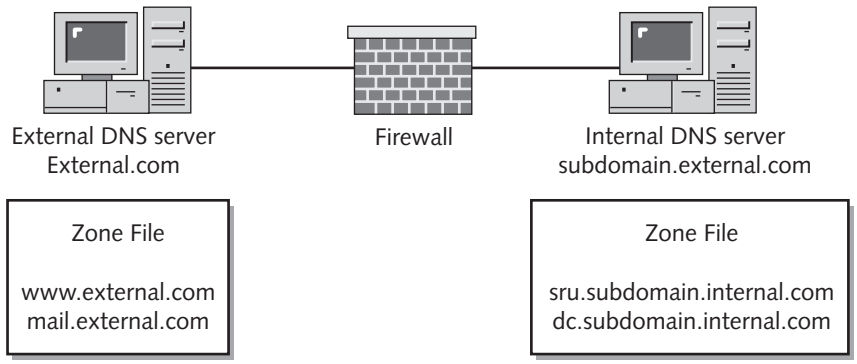

Figure 3-2 Extending a namespace

Using a contiguous namespace for both internal and external resources offers several advantages:

- Logon IDs and e-mail addresses are the same for the user base, thus eliminating that area of confusion.
- Internal and external resources can be accessed seamlessly by the user base.
- The Active Directory tree is the same for internal and external corporate resources.

Naturally, there are also some disadvantages:

- Administrators must be cautious not to accidentally publish internal resources on the external DNS server.
- Firewalls or other security products must be put in place to protect the internal network.

The ultimate decision about whether to create or extend a namespace will depend on the existing DNS configuration and the needs of the company. Regardless, a Windows 2000 DNS server is required for integration with Active Directory.

Site Design

As mentioned in Chapter 2, **sites** are areas of high-speed connectivity. Frequently, a site matches the physical location of a local area network (LAN). Within an enterprise network environment, these physical locations are connected via slower wide area network (WAN) links. Windows 2000 uses sites to control the bandwidth used by Active Directory replication. Active Directory tries to minimize latency within a site, and tries to minimize bandwidth utilization between sites.

The administrator for a network determines the number of sites and which domain controllers and IP subnets are associated with those sites. The actual implementation of the site structure is covered in Chapter 6 later in this book; this section will focus on the planning of sites. As an example of site planning, we will look at a real enterprise network environment and examine different site designs that may be applied to the environment.

The first element in site planning is determining which needs are the most important to the company. For example, if the ultimate goal is absolute ease of administration, perhaps a single site design is the most appropriate. If the design goal is controlling bandwidth utilization over every link, then it makes sense to generate a site for every physical location.

Let's take a look at the following network. The company (we will call it Rayco) manages stores in several cities and has a corporate office in Fort Worth. As shown in Figure 3-3, the company has 1.54 Mbps frame connections between Fort Worth, Dallas, Denver, and Houston. Several secondary sites exist within Houston and Denver: the Houston sites are all connected to the hub site via 384 Kbps metro frame connections, and the Denver sites are connected via 128 Kbps frame connections.

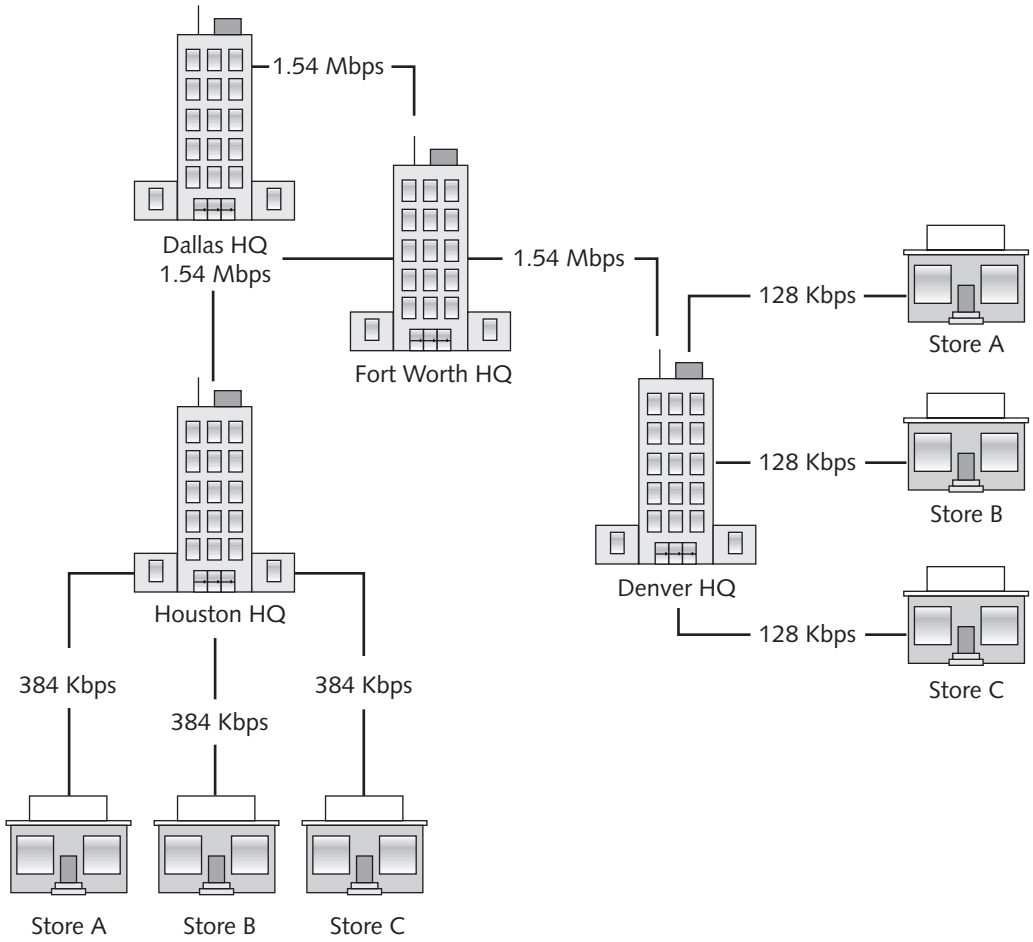

Figure 3-3 Rayco network connectivity

So, what possibilities are available with this environment? At a quick glance, it appears that many possibilities exist; the company could have from one to nine sites. Let's take a look at some of the more likely possibilities:

- *Single site:* One potential answer is to include the entire network within a single site. This approach would do much to ease administration, because there would be no need to create additional sites and site links. There would also be no need to move DCs between sites, because all the DCs would be part of the single default site. The problem with a single site is that domain replication traffic and authentication traffic are not controllable, and they could easily overwhelm some of the smaller WAN links. Even if a DC was placed at each physical location to handle authentication, the Active Directory replication alone could impact the remote sites in Denver.

- *Four sites:* Some elements of site design are impacted by the locations of the DCs. If the DCs were located only at the sites connected via the 1.54 Mbps links, the best configuration would generate four sites: Fort Worth and Dallas would each constitute a site, the Houston area locations would form the third site, and the Denver area locations would form the fourth. This design allows for better use of the long-haul links, while requiring a bare minimum of DCs.
- *Seven sites:* Even though a 1.54 Mbps connection is much slower than a LAN link, it still offers enough bandwidth that the physical location could be configured as a single site connected via frame connections. Obviously, with this structure the concern would be bandwidth utilization at the slower remote sites in Houston and Denver. Placing a DC at each of the slower locations and defining each of those locations as a site can overcome this issue. Doing so would allow the administrator to schedule replication with each of those slower sites. The administrator can schedule the replication to occur only at specified times, such as after business hours.
- *Nine sites:* If the company has the resources to place a DC at each site, then the optimal solution is to define each physical location as an independent site. Although doing so requires administrative overhead in order to define and maintain each site, the ability to control the replication and to authenticate locally result in the best performance for the Active Directory structure. Placing a DC at each physical location in our example results in nine sites. Of course, a site does not require that a DC be at that physical location—a site can consist of client machines only, which will then authenticate across the WAN link to the nearest DC.

A DC can be placed in multiple sites, if you wish to force clients to authenticate against a particular DC. To place a DC in multiple sites, first create the sites. Next, edit the Registry on the DC. Find the HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters subkey, and then add a REG_MULTI_SZ value named SiteCoverage. The names of the sites should be entered within the value.

In general, it is best to create as many sites as you have physical locations. In addition to the advantages we have already discussed, many of the services within Windows 2000 are **site aware**. A site-aware service will adjust its actions based upon the site from which the user logged in. This adjustment helps provide a seamless network experience regardless of the physical location of the user.

Domain Structure

Once the decisions have been made regarding name resolution and site design, it is time to think about domain structures. In the past, Windows NT domain structures have been influenced by two issues: First, any trust relationships were on a domain-by-domain basis

and were not transitive; and second, no way existed to grant administrative control over a section of a domain. As a result, any need to delegate administrative control almost always resulted in the creation of yet another domain.

The issues surrounding administrative control and resource allocation resulted in environments such as master logon domains with multiple trust relationships to the resource domain; or the ever-popular multi-master environment, in which multiple logon domains maintained a complex web of trust relationships with many resource domains. Windows NT administrators had their hands full designing and maintaining these trust relationships and troubleshooting problems with access rights.

Windows 2000 removes both of those limitations. Trusts are now automatic and transitive, so that the complex trust relationships common to NT environments are no longer required. In addition, a new structure known as an **Organizational Unit** (OU) allows Active Directory objects to be grouped together for administrative or policy purposes (we'll discuss OUs a bit later in the chapter).

From a strict technical perspective, you have very little reason to use multiple domains within a Windows 2000 environment. Because the OUs can function as a type of subdomain, the master-resource model is no longer needed to allow administrative control of a group of computers. This model was the most common reason for creating a multiple-domain environment when creating a domain from scratch.

Basically, a multiple-domain environment may be necessary under Windows 2000 for three reasons:

- *A very slow link exists between two or more physical locations*. Even though Windows 2000 is efficient at managing replication over site links, at absolute minimum a 128 Kbps connection is still needed for synchronous replication to operate effectively. If the physical locations are connected at a slower speed than 128 Kbps, it makes sense to create separate domains.
- *You must maintain a legacy Windows NT network structure*. Because Windows NT domains are not capable of a transitive trust, nor are they aware of Active Directory, the existing domain structure will need to stay in place until all the domains are upgraded.
- *Political considerations exist*. Although there may be no valid technical reason to create a separate domain, political considerations will play a role in the structure of the Windows 2000 environment. If domains that double as fiefdoms dominate the current network environment, it is unlikely that a single Windows 2000 domain will replace that structure.

A single-domain strategy is highly recommended. This strategy minimizes administrative overhead.

Uses of Organizational Units

Earlier, we defined an Organizational Unit as a grouping of Active Directory objects. We will discuss the implementation of OUs in Chapter 6; right now we will look at how OUs can be used within your domain structure.

It is important to understand two things about OUs before beginning to implement them within your environment:

- They are not required within a Windows 2000 environment. Access rights can be managed through security groups, much as they are in Windows NT.
- An OU is a domain object and cannot contain objects from another domain.

OUs function much like resource domains in Windows NT structures. Objects such as user accounts, computers, shares, printers, services, and more can be grouped together in an OU, and administrative rights can be granted to that OU by the domain administrator. This arrangement allows a departmental or geographical split on the security rights, while still avoiding the cumbersome and often unreliable trust links that joined the domains in a master-resource structure.

You can use several methods to implement OUs within a domain structure. Although OUs can be created and deleted with ease, proper planning will result in a structure that serves both the technical and business needs of the company. This planning process should include input from other departments within the company to help formulate the proper units and structure. A little extra time spent in planning will go a long way toward reducing problems after implementation. Some of the possible OU models are the following:

- *Object model:* Involves creating an OU for each type of object within the domain. This model is already implemented somewhat by default; the Users and Computers folders are simply OUs that are created automatically. Additional OUs can be created that contain printers, groups, and other objects. If necessary, secondary OUs can be created for more granularity, such as color printers or laptop computers. The advantage of this model is that it can easily be extended as new object types are added to the domain. The disadvantage is that usually no direct relationship exists between the object model and business processes within a company.
- *Departmental model:* Uses OUs to separate objects based upon the business departments associated with those objects. The departmental model groups users and the resources they most frequently use, such as shares, printers, and file servers. The advantage of this structure is the close integration of resources and the people who use them.
- *Geographic model:* Uses OUs to group objects based on the geographic location of the resources. Because OUs can be nested, the OUs can be as specific as a city or building, or as wide as a country. The geographic model can be used to cope with rapid changes in corporate structure, because user accounts and resources can be moved within the OUs as things change.

- *Administrative model:* Mimics the administrative structure within your organization. This model can be used to show the organizational structure of a company and can be nested through several levels to indicate the various levels of management. This model does not cope well with rapid changes within the company. If the changes are radical enough, many OUs may have to be scrapped and new ones built as replacements.
- *Business unit model:* Similar to the departmental model, but is based upon a much higher scale. Business units are usually divisions of a corporation that have a specific role and that often include multiple departments. A business unit model is generally used in conjunction with a departmental model to form a mirror of the corporate structure.

OUs can be used for many purposes within a Windows 2000 network structure. Primarily, you'll use OUs to provide structure for the resources within the Active Directory. If OUs are not used, the objects will be stored in a single list that can eventually become unmanageable. OUs also provide a flexible and easily managed way to handle permissions, especially if the company often undergoes structural changes. OUs can also be used to grant administrative control of resources such as computers or user accounts to a particular person or group or people, such as a departmental IT support organization.

Designing the Infrastructure

The underlying structure of a network impacts the placement of servers, DCs, and other resources. Likewise, the amount of resources at a physical location often impacts decisions about the allocation of bandwidth.

Windows 2000 replicates data much more efficiently than Windows NT has in the past. This additional efficiency exists for two main reasons:

- The data is compressed with replicating across WAN links between sites, whereas Windows NT treated all replication the same regardless of the speed between the Primary Domain Controller (PDC) and Backup Domain Controllers (BDCs).
- Windows 2000 replicates only the changes in an object, rather than the entire record for the object. This means, for example, that a password change for a user will replicate only the new password, not the entire user object.

Because of this additional efficiency, you usually don't need to upgrade if your current network environment is meeting the business needs of the company. In fact, with intersite replication and the ability to limit the replication to non-business hours, the network may function a bit better with Windows 2000 DCs rather than Windows NT systems.

The additional efficiency comes into play only after sites and site links have been configured within the Active Directory structure. As mentioned earlier in this chapter, it is

quite possible to create a multiple-location Active Directory structure that contains only a single site. However, a single site provides no advantage over the earlier versions of Windows NT—in fact, performance is likely to suffer, given that Windows 2000 attempts to minimize latency between DCs. However, we do not wish to form sites and throw DCs at random across the environment. Instead, you should follow a process to determine the proper placement of sites and to establish the impact on the existing infrastructure. The following sections describe this process.

Gather Data about the Network

The first element in any network planning exercise is to determine what elements the existing structure contains. Although this step may seem simplistic, many times an administrator will inherit a network that has little or no documentation. You must develop a map that includes all physical locations of a company, the current infrastructure layout between the locations, the speed and reliability of the infrastructure links, and the current utilization of those links. This map should also include information about the IP subnets in use on the network, if any exist.

Lay Out the Active Directory Sites

As we discussed earlier, best practices for Active Directory sites tell you to define a site for each physical location on the network. A site should be an area of high-speed connectivity, which usually means 10 Mbps LAN connections or higher. Take a look at the map created in the previous step and mark the areas that represent a concentration of computers or servers. These will be your sites.

Remember, sites and domains have no direct relationship to each other. A site can contain multiple domains, and a domain can cross multiple sites.

Place the DCs within the Sites

Once the sites are defined, it is time to determine how many DCs are required and where they should be located. Remember that not all sites require a DC—a site can be composed entirely of client computers. Also remember that the more DCs exist, the more replication overhead the network will suffer.

The first step is to determine where the DCs should be located. It is tempting to simply install a DC in each site; but you should consider the following several reasons to locate a DC at a site:

- *A slow bandwidth link exists to the nearest DC.* If a site has a fast link to the nearest DC, then it is possible to authenticate across the link. However, if the site is connected via a low-bandwidth link, then authentication across that link will be slow. Placing a DC at that location will dramatically improve authentication times.

- *A domain is limited to a particular physical location*. In this case, you don't need to pass authentication traffic across a WAN link when the DC can be located at the physical site.
- *Users at a site perform a large number of cross-domain searches*. In this case, a DC doubling as a global catalog server would provide the best performance for these searches.
- *You want to speed authentication*. More-than-sufficient bandwidth may be available to access a central DC, but performance will always be quicker with a local DC.

A DC at a site may also be a poor idea for several reasons. Some of these reasons are listed here:

- *Hardware costs:* Although we hope this will not be an issue, it can be expensive to place a server-class machine at each site, especially when the site has few users.
- *Physical security:* If you can't physically secure a DC at the site, then it may be prudent not to locate a DC at that site. Many of the Windows NT security exploits require console access to a DC, and it is reasonable to expect similar exploits to arise with Windows 2000.
- *Administrative overhead:* Although Windows 2000 offers much more remote management capability than previous versions of Windows NT, every additional DC will result in an added load on the IT support staff. Consolidating the number of DCs will result in a more manageable environment.
- *Replication overhead:* As the number of DCs increases, so does the replication traffic for the domain.

Once you have decided where your sites and DC will be placed, you should have a good idea of the loads placed upon your network. Compare the locations of the DC and the large sites with the bandwidth links and speeds collected earlier. You should notice that the higher-speed links tend to be associated with the DC locations. If you find a major discrepancy, then you either need to increase the bandwidth at that site or revisit the decisions about sites and DCs.

Establish Replication Schedules

The replication schedule also impacts the infrastructure. Replication can be limited to particular times, so that the replication operation does not affect the users who need to use the bandwidth for business purposes. We will discuss the mechanics of limiting bandwidth later in this book; at this point, we are discussing strategies for optimizing replication traffic.

Forcing replication to occur outside of normal business hours increases the effective bandwidth of a remote site. For sites that are connected with high-speed links, the effect of replication every three hours (the default interval) may be minimal. Sites that are connected via slow links may see a degradation of performance, especially if many regular changes occur in the Active Directory objects.

A good rule of thumb for replication traffic is that the slower the link, the more restrictive the replication schedule should be:

- *High bandwidth (low cost):* Replication should be allowed throughout the day. The default interval is three hours between replication attempts.
- *Medium bandwidth (medium cost):* Replication may be restricted to evening hours. The default interval may be changed to lengthen the time between replication attempts.
- *Low bandwidth (high cost):* Replication should be restricted to a particular window of time. It is important that this window of time match the replication times available at the other end of the site link. If the replication windows do not match, replication cannot occur.

The combination of physical connectivity, site design, DC placement, and replication schedules will determine how well your network performs. Although a WAN never has enough bandwidth, judicious use of replication schedules can minimize the impact of replication on the network. Windows 2000's use of sites actually places a lighter load on the network infrastructure than an equivalent Windows NT structure. If the existing network infrastructure is supporting a Windows NT environment, then it will probably be able to support a Windows 2000 environment without problems. Naturally, it is important to verify the network structure before implementing any new network operating system.

Chapter Summary

- Planning remains the most important element in designing and implementing a Windows 2000 networking environment. The Active Directory service requires much more planning than the Windows NT operating system, due to elements such as sites, site links, and replication scheduling.
- The namespace is the first issue you will face in planning the new Windows 2000 implementation. Windows 2000 uses DNS naming rather than the NetBIOS naming that dominates Windows NT networking. The DNS naming requires a fully qualified domain name for the Windows domain, such as Microsoft.com.
- Companies that have not used DNS previously must develop a DNS solution for internal name resolution. The domain that a company wishes to use must be registered with an ICANN-approved registrar to prevent it being used by

some other company. Domain names can be registered either directly by a company or through an ISP or other connectivity provider. Once the name has been registered, it may be used.

- Several options are available for companies that previously had a registered DNS domain name for either internal or external resources. One option is to register another domain name for internal use only. This option provides additional security, because there is no need to publish the internal DNS information to the outside world. The negatives are minor: primarily, the need to maintain an additional domain name and the administrative overhead that comes with that additional name.
- A company can also extend a domain name to include the new internal resources. The most common method is to create a subdomain within the domain name and use that subdomain for internal resources. As an example, TexasPinball.com could use an internal subdomain such as Corporate.TexasPinball.com for its Active Directory structure. The problem with using a subdomain is maintaining a separation between internal and external resources through zone files and firewall configurations. It is important not to publish information about internal resources on any DNS server reachable from the outside world.
- Once the decision is made regarding the namespace, the next level of planning involves determining how many domains will be required in the new Windows 2000 structure. Windows 2000 offers some new elements that can minimize the number of domains. Organizational Units (OUs) can be configured to perform many of the same functions as resource domains. In general, strive for the fewest as possible domains in an environment. It is recommended that a single domain be used unless political or legacy issues require a multiple-domain structure.
- OUs are new with Windows 2000. An OU is essentially a container than can include other objects within the domain. An OU cannot include objects from another domain. OUs can be nested within each other as necessary. Administrative control over an OU can be granted to a domain user or to a group of domain users. Doing so allows an OU to function as a resource domain and to be controlled on an individual basis within the domain.
- You can use several OU models to organize OUs within a domain. Some of these methods include the geographic model, business unit model, administrative model, departmental model, and object model. Each model has advantages and disadvantages. In order to develop an OU structure that best fits your company, other departments should be allowed to provide significant input. Remember, the goal is to reduce the effort needed to maintain the structure and to allow for flexibility if the company reorganizes.
- Infrastructure issues are always a concern when a new product is introduced on a network. This is a great time to verify that the network infrastructure matches

the information you have regarding speed, subnet allocation, and routes. The major concern is whether the additional load will adversely affect the ability of the company to perform its primary function. Fortunately, Windows 2000 is better at managing replication bandwidth than its predecessor, and replication can be scheduled so that it will not affect the users at a location.

- The amount of bandwidth used by replication is dependent upon a number of items. The primary factors are the number of sites and the number of DCs within the Active Directory structure. The structure of a company's network will determine the number of sites. In general, a site should be created for each subnet or physical location.
- The number of DCs will be determined by several factors. The first is the available bandwidth between the clients and the DCs. Not every site will require a DC, if sufficient bandwidth exists to allow reasonably quick authentication via another DC. If the bandwidth is restricted to a site, however, a DC at that site makes perfect sense. The second factor is the relative value of a DC versus the additional hardware costs and administrative headaches associated with additional servers at remote locations.
- Replication traffic can be controlled through properties of the site links. Links can be scheduled to be active only at certain times. Replication traffic will not flow while a site link is inactive, but normal network traffic will be allowed. Sites that are connected via high-bandwidth links should not be restricted, whereas sites that have very low bandwidth should be limited to a particular replication time.